Constructions of quantum codes

Petr Lisoněk
Simon Fraser University
Burnaby, BC, Canada

joint work with Reza Dastbasteh

The 3rd International Workshop
on Boolean Functions and their Applications (BFA)
Loen, Norway

20 June 2018

Abstract

We review methods for constructing quantum codes from classical additive and linear codes that are self-orthogonal with respect to the symplectic inner product on the ambient vector space. We generalize these constructions to codes that are nearly self-orthogonal. The families of codes considered include additive cyclic codes, twisted codes, linear cyclic and constacyclic codes and duadic codes. We review the known techniques for bounding the minimum distance of cyclic codes and we show new applications of these techniques to twisted codes. We illustrate the applicability of our methods by presenting many new examples of quantum codes that have higher minimum distance than the previously known codes.

Notation

$\mathbb{F}_{2^n} = \mathrm{GF}(2^n)$

$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ where $\omega^2 = \omega + 1$

$\mathrm{Tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{im}}$ ... trace from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$

$\mathrm{Tr}(x) = \mathrm{Tr}_1^n(x)$ ... absolute trace

For $x, y \in \mathbb{F}_4^n$
$\langle x, y \rangle_h = \sum_{i=1}^n x_i \overline{y_i} = \sum_{i=1}^n x_i {y_i}^2$ ... Hermitian inner product
$\langle x, y \rangle_s = \mathrm{Tr}(\langle x, y \rangle_h)$ ... symplectic inner product

$C^{\perp_h} := \{u \in \mathbb{F}_4^n : (\forall x \in C) \langle u, x \rangle_h = 0\}$ ... Hermitian dual of C

$C^{\perp_s} := \{u \in \mathbb{F}_4^n : (\forall x \in C) \langle u, x \rangle_s = 0\}$ ... symplectic dual of C

Quantum codes

A *quantum error-correcting code* is a code that protects quantum information from corruption by noise (decoherence) on the quantum channel in a way that is similar to how classical error-correcting codes protect information on the classical channel.

We denote by $[[n, k, d]]$ the parameters of a binary quantum code that encodes k logical qubits into n physical qubits and has minimum distance d. We only deal with *binary* quantum codes in this talk, but the methods can be generalized to odd characteristic as well.

For fixed n and k, the higher d is, the more error control the code achieves.

Stabilizer quantum codes

A binary stabilizer quantum code of length n is equivalent to a quaternary additive code (an additive subgroup) $C \subset \mathbb{F}_4^n$ such that $\langle x, y \rangle_s = 0$ for all $x, y \in C$.

A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane, Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory* 1998, and some earlier papers.

Theorem

Given a self-orthogonal additive $(n, 2^{n-k})$ code C (i.e. $C \subseteq C^{\perp_s}$) such that there are no vectors of weight less than d in $C^{\perp_s} \setminus C$, we can construct an $[[n, k, d]]$ quantum code.

C is *pure* if there are no non-zero vectors of weight less than d in $C^{\perp_s}$.

Stabilizer quantum codes

In the special case $k = 0$, we define $d = \min\{\mathrm{wt}(u) : u \in C \setminus \{0\}\}$ and C is *self-dual* i.e. $C = C^{\perp_s}$.

If we restrict our attention to $\mathbb{F}_4$-linear subspaces of $\mathbb{F}_4^n$, then the following theorem expresses the parameters of the quantum code that can be constructed from a classical linear, Hermitian dual containing quaternary code.

Theorem

Given a linear $[n, k, d]_4$ code C such that $C^{\perp_h} \subseteq C$, we can construct an $[[n, 2k - n, d]]$ quantum code.

Stabilizer quantum codes

Theorem

Let C be an $[[n, k, d]]$ code.
a) If $k > 0$, then there exists an $[[n+1, k, d]]$ code.
b) If $n \neq 1$ and C is pure, then there exists an $[[n-1, k+1, d-1]]$ code.
c) If $k > 1$ or if $k = 1$ and the code is pure, then there exists an $[[n, k-1, d]]$ code.
d) If $n \geq 2$ then $[[n-1, k, d-1]]$ code exists.

Quantum codes from nearly self-orthogonal linear codes

Theorem (L., Singh 2014)

For an $[n,k]_4$ linear code C denote $e := n - k - \dim(C \cap C^{\perp_h})$. Then there exists an $[[n+e, 2k-n+e, d]]$ quantum code with $d \geq \min\{\mathrm{wt}(C), \mathrm{wt}(C + C^{\perp_h}) + 1\}$.

Note that for $e = 0$ we get the standard construction mentioned earlier.

Quantum codes from nearly self-orthogonal additive codes

Lemma

For any additive code $C \subseteq \mathbb{F}_4^n$ *let* $2k := \dim_{\mathbb{F}_2}(C) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_s})$. *We can find vectors* $B_1, B_2, \ldots, B_{2k} \in C \setminus (C \cap C^{\perp_s})$ *such that* $\langle B_{2i-1}, B_{2i} \rangle_s = 1$ *and* $\langle B_{2i-1}, B_j \rangle_s = \langle B_{2i}, B_m \rangle_s = 0$ *for* $1 \leq i \leq k$, $j \neq 2i$, *and* $m \neq 2i - 1$.

Lemma

Let C *be an* $(n, 2^\ell)$ *additive code over* $\mathbb{F}_4$ *and* $2k := \dim_{\mathbb{F}_2}(C) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_s})$. *We can extend* C *to a new code* Q, *which is an* $(n + k, 2^\ell)$ *self-orthogonal* ($Q \subseteq Q^{\perp_s}$) *additive code over* $\mathbb{F}_4$.

Proof: Suppose C is an additive code with the mentioned properties and $\dim_{\mathbb{F}_2}(C) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_s}) = 2k$. Let $G = \begin{bmatrix} M \\ B \end{bmatrix}$ be a generator matrix for C, where the last $2k$ rows are in $C \setminus (C \cap C^{\perp_s})$, in the form as in previous lemma, and other rows form a basis for $C \cap C^{\perp_s}$. Let T be a matrix such that $T_{2j-1,j} = 1$ and $T_{2j,j} = \omega$ for $1 \leq j \leq k$, and the other entries of T are zero. The matrix

$$G' = \begin{bmatrix} M_{s \times n} & 0_{s \times k} \\ B_{2k \times n} & T_{2k \times k} \end{bmatrix}$$

where $s = \dim_{\mathbb{F}_2}(C \cap C^{\perp_s})$ generates an $(n + k, 2^\ell)$ additive code Q over $\mathbb{F}_4$ and one can easily see that $Q \subseteq Q^{\perp_s}$.

Quantum codes from nearly self-orthogonal additive codes

Theorem

Let C be an $(n, 2^k)$ additive code over $\mathbb{F}_4$ and

$$e = \frac{2n - k - \dim_{\mathbb{F}_2}(C \cap C^{\perp_s})}{2}.$$

There exists an $[[n + e, k - n + e, d]]$ quantum code with $d \geq \min\{\mathrm{wt}(C), \mathrm{wt}(C + C^{\perp_s}) + 1\}$.

Proof: We note $\dim_{\mathbb{F}_2}(C^{\perp_s}) = 2n - k$. Let $e = \frac{2n-k-\dim_{\mathbb{F}_2}(C \cap C^{\perp_s})}{2}$ and $\dim_{\mathbb{F}_2}(C \cap C^{\perp_s}) = s$.

Let $r(Z)$ denote the set of rows of matrix Z. Consider the matrix

$$G = \begin{bmatrix} M_{s\times n} & 0_{s\times e} \\ A_{(k-s)\times n} & 0_{(k-s)\times e} \\ B_{2e\times n} & T_{2e\times e} \end{bmatrix}$$

where $r(M)$ is a basis for $C \cap C^{\perp_s}$, $r(A) \cup r(M)$ is a basis for C, $r(B) = B_1, B_2, \cdots, B_{2e}$, where $\langle B_{2i-1}, B_{2i}\rangle_s = 1$ and $\langle B_{2i-1}, B_p\rangle_s = \langle B_{2i}, B_q\rangle_s = 0$ for $1 \leq i \leq e$, $p \neq 2i$, and $q \neq 2i-1$. Also, the set $r(B) \cup r(M)$ is a basis for $C^{\perp_s}$, and T is the matrix which was introduced in the proof of the previous lemma.

Quantum codes from nearly self-orthogonal additive codes

Let E be the additive code generated by the matrix G. Consider the code generated by

$$S = \begin{bmatrix} M_{s\times n} & 0_{s\times e} \\ B_{2e\times n} & T_{2e\times e} \end{bmatrix}.$$

By construction and the above Lemma, rows of S are orthogonal to the rows of G. Moreover, $\dim_{\mathbb{F}_2}(E) = 2n - s$ and $\dim_{\mathbb{F}_2}(E^{\perp_s}) = s + 2e$. Therefore, S is a generator matrix for the code $E^{\perp_s}$ and $E^{\perp_s} \subseteq E$. Hence $E^{\perp_s}$ is an $(n+e, 2^{2e+s}) = (n+e, 2^{2n-k}) = (n+e, 2^{(n+e)-(k-n+e)})$ self-orthogonal code which determines an $[[n+e, k-n+e]]$ quantum code.

It remains to find the bound for minimum distance. Let $x = (x_1, x_2) \in E$, where $x_1 \in \mathbb{F}_4^n$ and $x_2 \in \mathbb{F}_4^e$. So x is linear combination of rows of G. If no row of B appears in the linear combination, then $\mathrm{wt}(x) \geq \mathrm{wt}(C)$. If some of the rows of B enter this linear combination, then $\mathrm{wt}(x) \geq \mathrm{wt}(C + C^{\perp_s}) + 1$.

Twisted codes

J. Bierbrauer, Y. Edel, Quantum twisted codes. Journal of Combinatorial Designs 2000.

Let $F = \mathbb{F}_{q^r}$ and let E be a two-dimensional $\mathbb{F}_q$-vector space. Let $\phi : F \to E$ be a surjective $\mathbb{F}_q$-linear map with $\phi(x) = (\mathrm{Tr}(x), \mathrm{Tr}(\gamma x))$, where $\gamma \in F \setminus \mathbb{F}_q$ and $\kappa = [\mathbb{F}_q(\gamma) : \mathbb{F}_q]$. For any divisor $n|q^r - 1$, F^* contains a unique subgroup of order n which we denote by W. For a given subset $A \subseteq \mathbb{Z}/n\mathbb{Z}$, define $P(A) := \{\sum_{i \in A} a_i x^i : a_i \in F\}$. Let $B(A)$ be the matrix, where the rows and columns are indexed by $P(A)$ and W respectively. The entry in the row $p(x)$ and the column u is $p(u)$.

Let $V = E^n$ be a $2n$-dimensional $\mathbb{F}_q$-vector space endowed with a symplectic bilinear form $\langle , \rangle_s$. We call the dual of the code generated by the rows of $\phi(B(A))$ a **twisted code** with the defining set A and denote it by $\mathcal{C}(A)$.

Twisted codes

Twisted codes are $\mathbb{F}_q$-linear (additive) cyclic codes over $E \simeq \mathbb{F}_{q^2}$.

Throughout let Z denote a q-cyclotomic coset modulo n. Recall that A is the defining set of the code $\mathcal{C}(A)$. We call $Z \cap A \neq \emptyset$ *unsaturated* if $\kappa \mid |Z|$ and for any $aq^i, aq^j \in Z \cap A$ we have $\kappa | i - j$.

The dimension of $\mathcal{C}(A)$ is $\sum_Z c_Z(A)$, where the sum runs over all cyclotomic cosets Z and

$$c_Z(A) = \begin{cases} 2|Z| & \text{if } Z \cap A = \emptyset \\ |Z| & \text{if } Z \cap A \text{ is unsaturated} \\ 0 & \text{if } Z \cap A \text{ is saturated} \end{cases}$$

Twisted codes

Suppose $Z \cap A$ is unsaturated and $a \in Z \cap A$. By $(Z \cap A)^H$ we denote the set of all elements $aq^i \in Z$ such that $\kappa | i$.

By extending the defining set A to

$$\tilde{A} = \bigcup_{Z \cap A \ Sat} Z \bigcup_{Z \cap A \ Usat} (Z \cap A)^H$$

we obtain the same code as $\phi(B(A))$. From now on, we consider $\tilde{A}$ as the defining set of the code $\mathcal{C}(A) = (\phi(B(A)))^{\perp_s}$.

The maximum defining set for $\phi(B(A))$ is

$$A^{\perp} = \bigcup_{Z \cap A = \emptyset} -Z \bigcup_{Z \cap A \ Usat} -((Z \cap A)^H).$$

Twisted codes

We call the cyclotomic coset Z *purely unsaturated* if $Z \cap A$ and $-Z \cap A$ are unsaturated and $(Z \cap A)^H = -((-Z \cap A)^H)$.

Proposition

Let A be the defining set of $\mathcal{C}(A)$. Then $\phi(B(A)) + \mathcal{C}(A)$ is a twisted code and its defining set is

$$B^\perp = \bigcup_{Z \cap A \ PUsat} (Z \cap A)^H \bigcup_{\substack{Z' \cap A = \emptyset \\ -Z' \cap A \ Sat}} -Z' \bigcup_{\substack{Z' \cap A = \emptyset \\ -Z' \cap A \ Usat}} (-Z' \cap A)^H$$
$$\bigcup_{\substack{Z' \cap A \ Sat \\ -Z' \cap A \ Usat}} (Z' \cap A)^H \bigcup_{Z' \cap A \ PUsat} (Z' \cap A)^H,$$

where Z runs over all the cyclotomic cosets with $Z = -Z$ and Z' runs over all the cyclotomic cosets with $Z' \neq -Z'$.

Twisted codes

The previous proposition is useful for determining a bound for minimum distance of $\phi(B(A)) + \mathcal{C}(A)$ (details to follow) which in turn is used in bounding the minimum distance of codes arising from our construction given above.

We slightly reformulate the known condition for self-orthogonality of twisted code.

Corollary

Let A be the defining set for the twisted code $\mathcal{C}(A)$. Then $\phi(B(A))$ is self-orthogonal if and only if for every Z with $Z \cap A \neq \emptyset$ one of the following cases occurs:
1) $Z \cap A$ is purely unsaturated
2) $-Z \cap A = \emptyset$

Twisted codes

We also can find the parameter $e = \frac{\dim(C^{\perp}) - \dim(C \cap C^{\perp})}{2}$ which is used in our construction.

Corollary

Let A be the defining set for the twisted code $\mathcal{C}(A)$. Then

$$\dim(\phi(B(A))) - \dim(\mathcal{C}(A) \cap \phi(B(A))) =$$

$$\sum_{Z_i \cap A \ Sat} 2s_i \ + \sum_{\substack{Z_i \cap A \ Usat \\ (Z_i \cap A)^H \neq -((Z_i \cap A)^H)}} s_i \ + \sum_{\substack{Z_i' \cap A \ Sat \\ -Z_i' \cap A \ Sat}} 4s_i'$$

$$+ \sum_{\substack{Z_i' \cap A \ Sat \\ -Z_i' \cap A \ Usat}} 2s_i' \ + \sum_{\substack{-Z_i' \cap A \ Sat \\ Z_i' \cap A \ Usat}} 2s_i' \ + \sum_{\substack{Z_i' \cap A \ Usat \\ -Z_i' \cap A \ Usat \\ (Z_i' \cap A)^H \neq -((-Z' \cap A)^H)}} 2s_i',$$

where $Z_i = -Z_i$, $Z_j' \neq -Z_j'$, $s_i = |Z_i|$, $s_i' = |Z_i'|$.

Twisted codes

In particular, the case $e = 1$ occurs iff all the cyclotomic cosets Z such that $Z \cap A \neq \emptyset$ satisfy one of the conditions of the earlier corollary, except one cyclotomic coset which is a singleton, or $\kappa = 2$, $Z \cap A = \{a\}$, and $Z = \{a, n - a\}$.

Bounds on minimum distance

We show that several bounds on minimum distance of linear codes can be extended to twisted codes.

Definition

A set $\{i_1, i_2, \ldots, i_r\} \subseteq \mathbb{Z}/n\mathbb{Z}$ is called *consecutive set* or *interval* of length r if there exists $c \in \mathbb{Z}/n\mathbb{Z}$ with $(c, n) = 1$ such that $\{ci_1, ci_2, \ldots, ci_r\} = \{j, j+1, j+2, \ldots, j+r-1\} \pmod{n}$.

Theorem (Bierbrauer & Edel 1997, BCH bound for twisted codes)

Let A be the defining set of a twisted code $\mathcal{C}(A)$ such that A contains an interval of length $t-1$. Then $d_{\mathcal{C}(A)} \geq t$.

Bounds on minimum distance

For $X, Y \subset \mathbb{Z}/n\mathbb{Z}$ let $X + Y := \{x + y : x \in X,\ y \in Y\}$.

Theorem (Hartmann-Tzeng Bound for twisted codes)

Let A be the defining set of a twisted code $\mathcal{C}(A)$ such that A contains $l_1 + l_2$ where l_1, l_2 are intervals. Then $d_{\mathcal{C}(A)} \geq |l_1| + |l_2|$.

This theorem generalizes to the sum of more than two intervals, and the gcd condition can be relaxed.

Bounds on minimum distance

Theorem (Roos Bound for twisted codes)

Let M, N be non-empty subsets of $\mathbb{Z}/n\mathbb{Z}$ and suppose that N is an interval. If there exists an interval $\bar{M} \subseteq \mathbb{Z}/n\mathbb{Z}$ where $M \subseteq \bar{M}$ and $|\bar{M}| \leq |M| + |N| - 1$, then $d_{\mathcal{C}(M+N)} \geq |M| + |N|$.

Bounds on minimum distance

Theorem

Let A be the defining set of the twisted code $\mathcal{C}(A)$. If the linear cyclic code over F with the the defining set A has minimum distance d, then $\mathcal{C}(A)$ has minimum distance $\geq d$.

Hence also other bounds known for linear codes, in particular van Lint-Wilson bounds, apply to twisted codes.

Constacyclic codes

Definition

Let $\lambda \in \mathbb{F}_4^*$ and $C \subseteq \mathbb{F}_4^n$. We say that C is a *constacyclic code* if for every $(x_0, \ldots, x_{n-1}) \in C$ we have $(\lambda x_{n-1}, x_0, \ldots, x_{n-2}) \in C$.

Duadic codes

Duadic codes are generalizations of quadratic residue codes. Binary duadic codes were initially defined by Leon, Masley and Pless in 1984 and later generalized to arbitrary fields.

Definition

Let C_1 and C_2 be linear cyclic codes of length n over $\mathbb{F}_q$ with defining sets $T_1 = \{0\} \cup S_1$ and $T_2 = \{0\} \cup S_2$ where $0 \notin S_1 \cup S_2$. We say that C_1 and C_2 are a pair of duadic codes if $S_1 \cup S_2 = \{1, \ldots, n-1\}$ and $S_1 \cap S_2 = \emptyset$ and there exists a multiplier μ such that $S_1\mu = S_2$.

New quantum codes

Quantum codes listed in the next slides have a *higher* minimum distance than the best known codes listed at `http://codetables.de/` (M. Grassl, Tables of linear codes and quantum codes).

Secondary constructions applied to these new codes produce many more record breaking codes.

New quantum codes

Linear cyclic codes

e=1

$[52, 10, 11]]$
$[[86, 36, 12]]$
$[[86, 40, 11]]$
$[[94, 52, 9]]$
$[[94, 62, 7]]$

New quantum codes

Twisted cyclic codes

e=0

$[[57, 3, 14]]$ (generalized duadic)
$[[63, 42, 6]]$
$[[69, 3, 16]]$
$[[73, 46, 7]]$
$[[73, 55, 5]]$ (Melas type)
$[[79, 40, 9]]$
$[[89, 45, 10]]$
$[[91, 61, 7]]$
$[[93, 63, 7]]$
$[[97, 49, 10]]$
$[[105, 61, 9]]$

New quantum codes

Twisted cyclic codes

e=1

$[[46, 18, 8]]$
$[[58, 20, 10]]$
$[[64, 53, 4]]$
$[[74, 45, 7]]$
$[[80, 39, 9]]$
$[[92, 60, 7]]$
$[[94, 62, 7]]$

New quantum codes

Linear constacyclic codes

e=0
$[[39, 3, 11]]$
$[[105, 21, 17]]$
$[[105, 33, 14]]$
$[[105, 45, 12]]$
$[[105, 51, 11]]$

e=1
$[[86, 12, 18]]$
$[[86, 28, 14]]$
$[[86, 36, 12]]$
$[[86, 40, 11]]$
$[[92, 24, 16]]$

e=3
$[[108, 30, 15]]$

New quantum codes

Duadic codes

$e = 1$, Hermitian self-dual codes. These are widely studied objects whose importance extends beyond quantum codes.

$[[110, 0, 22]]$
(best known $[[110, 0, 19]]$)

$[[114, 0, \geq 22]]$ ... $[[114, 0, 26]]$ (?)
(best known $[[114, 0, 18]]$)

$[[120, 0, 20]]$
(best known $[[120, 0, 18]]$)

The 14th International Conference on Finite Fields and Their Applications (Fq14)

3–7 June 2019, Vancouver, Canada

Fq14 website

https://www.sfu.ca/math/Fq14